Методи цифрового захисту графічних зображень

Євгенія Шабала[1], *Анастасія Латанська*[2]

Київський національний університет будівництва і архітектури (КНУБА)
Повітрофлотський проспект, 31, Київ, Україна, 03037
[1]wild_miledi@ukr.net, https://orcid.org/0000-0002-0428-9273
[2]zmei.kira.lanska@gmail.com, https://orcid.org/0000-0003-3719-1229

Отримано 28.04.2021, прийнято 19.05.2021
https://doi.org/10.32347/tit2141.0305

ВСТУП

Швидкий розвиток, широке поширення інформаційних і комунікаційних технологій в наш час, легкість передачі і поширення інформації в комп'ютерних мережах тягнуть за собою необхідність захисту файлів що публікуються у відкритому доступі або переданих по мережі документів. Забезпечення надійної передачі і зберігання інформації передбачає два аспекти: по-перше, запобігання несанкціонованого доступу до даних і, по-друге, забезпечення надійної передачі даних незважаючи на перешкоди.

МЕТА І МЕТОДИ ДОСЛІДЖЕННЯ

Для запобігання несанкціонованого вторинного використання даних, їх модифікації та порушення авторського права, а також незаконного поширення цих даних, використовуються різні технічні пристосування, в залежності від типу переданих даних (наприклад, можливість читання документа при одночасній забороні редагування). Одним з видів такого захисту зокрема, для мультимедійних файлів є впровадження водяних знаків (watermark injection). Водяні знаки однозначно ідентифікують власника мультимедійного файлу, при цьому вони забезпечують можливість підтвердження авторства в будь-який момент використання медіафайлу.

РЕЗУЛЬТАТИ ТА ОБГОВОРЕННЯ

Водяні знаки можуть бути впроваджені в будь-який мультимедійний документ (оригінал, звук, відео і т. д.) і при необхідності підтвердити відповідність медіафайлу оригіналу.

Основні вимоги, що пред'являються до водяних знаків: надійність і стійкість до спотворень, непомітності, робастности до обробки сигналів (robust - здатність системи до відновлення після впливу на неї зовнішніх/внутрішніх спотворень, в тому числі умисних). ЦВЗ мають невеликий обсяг, але для виконання зазначених вище вимог, при їх встановленні використовуються більш складні методи, ніж для вбудовування звичайних заголовків або повідомлень.

Зазвичай цифрові водяні знаки невидимі (методи LSB і Patchwork). Однак ЦВЗ можуть бути видимими на зображенні або відео. Зазвичай це інформація являє собою текст або логотип, який ідентифікує автора (методи мікшування і нанесення тексту).

Метод мікшування передбачає нанесення одного зображення на інше в певному співвідношенні. Цей алгоритм найбільш близький до класичних водяних знаків, тому що являє собою накладення двох зображень, одне з яких свідчить про справжність зображення. Як зображення може бути, наприклад, логотип фірми або сайту - власника зображення.

Так званий, життєвий цикл ЦВЗ може бути описаний таким чином. Спочатку в сигнал-джерело S в довіреному середовищі впроваджуються водяні знаки за допомогою функції E. В результаті виходить сигнал SE. Наступний етап - поширення SE через мережу або будь-яким іншим способом. Під час поширення на сигнал може бути здійснена атака. У отриманого сигналу SEA водяні знаки можуть бути потенційно знищені або змінені. На наступному

етапі функція виявлення D намагається виявити водяні знаки w, а функція R витягнути з сигналу впровадження повідомлення. Цей процес потенційно може здійснювати зловмисник. Схема життєвого циклу ЦВЗ показана на Рис. 1.

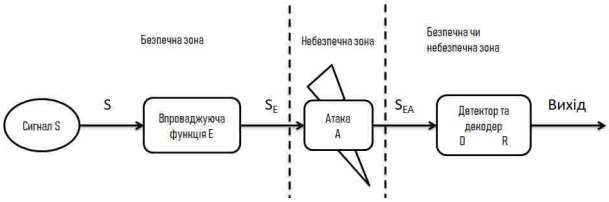

Рис. 1. Життєвий цикл ЦВЗ

Алгоритм методу мікшування полягає в наступному. Спочатку розраховується розташування водяного знаку на контейнері. Після цього відбувається розрахунок коефіцієнтів стиснення ЦВЗ по відношенню до контейнера, і після цього попіксельно наноситься водяний знак.

Водяний знак, нанесений методом мікшування, завжди видно неозброєним оком і не може бути вилучений з зображення, якщо в наявності немає файлу з ЦВЗ.

Метод нанесення тексту відноситься до найбільш часто використаних. В заданій точці на поверхню зображення наноситься текст різного ступеня прозорості, з різними атрибутами. Більшість зображень, які розповсюджуються через інтернет, мають такий водяний знак,

найчастіше це адреса сайту або ім'я автора. Неможливість видалення даного ЦВЗ підтверджується тими ж викладками, що і для методу мікшування.

Водяні знаки, нанесені цими методами, є надійними: видалити їх можна, тільки знищивши саме зображення.

При впровадженні ЦВЗ використовується співвідношення:

$$\tilde{n}_R = \mathrm{mix}((c_0.\alpha \cdot T + c_1.\alpha \cdot (1-T)),(c_0.R \cdot T + c_1.R \cdot (1-T)),$$
$$(c_0.G \cdot T + c_1.G \cdot (1-T)),(c_0.B \cdot T + c_1.B \cdot (1-T))),$$

де $\tilde{n}_R$- результуюче значення пікселя, $\tilde{n}_0$- початкове значення пікселя вихідного зображення, $\tilde{n}_1$ - значення відповідного пікселя ЦВЗ, T - коефіцієнт прозорості.

Припустимо, що є зображення з впровадженим водяним знаком. Тоді для отримання початкового зображення необхідно вирішити систему з 4 рівнянь:

$$\tilde{n}_R.a = c_0.a \times T + c_1.a \times (1-T);$$
$$\tilde{n}_R.R = c_0.R \times T + c_1.R \times (1-T);$$
$$\tilde{n}_R.G = c_0.G \times T + c_1.G \times (1-T);$$
$$\tilde{n}_R.B = c_0.B \times T + c_1.B \times (1-T),$$

що можливо, тільки маючи в наявності файлу із зображенням ЦВЗ, що може зробити тільки автор зображення.

Метод LSB заснований на тому факті, що при оцифрування зображення або звуку завжди присутня похибка дискретизації, рівна найменшому значущому розряду числа, що визначає величину колірної складової елемента зображення або амплітуди звукового сигналу. Тому заміна найменш значущих бітів прихованим повідомленням в більшості випадків не викликає значної трансформації сигналу і не виявляється візуально чи аудально. Займаючи два біта з восьми на кожен канал, ми будемо мати можливість заховати три байта корисної інформації на кожні чотири пікселя зображення, що відповідає 25% обсягу картинки. Таким чином, маючи файл зображення розміром 200 Кбайт, ми можемо приховати в ньому до 50 Кбайт довільних даних так, що неозброєним оком ці зміни не будуть помітні.

В якості водяного знаку метод LSB використовується наступним чином. Власник файлу впроваджує водяний знак шляхом запису в нього інформації з певного файлу. Якщо виникла необхідність підтвердити авторство, власник отримує інформацію з контейнера і доводить тотожність витягнутого і пред'явленого файлів, що однозначно говорить про авторство.

В якості водяного знаку метод LSB використовується наступним чином. Власник файлу впроваджує водяний знак шляхом запису в нього інформації з певного файлу. Якщо виникла необхідність підтвердити авторство, власник отримує інформацію з контейнера і доводить тотожність витягну-

того і пред'явленого файлів, що однозначно говорить про авторство.

Даний ЦВЗ є крихким: навіть перетворення в стислий формат знищує його повністю. Метод Patchwork заснований на внесення змін в дві ділянки зображення: на ділянці А яскравість зображення незначно збільшується, а на ділянці В - зменшується.

Наявність подібного відхилення від очікуваного значення свідчить про наявність вбудованої в зображення мітки. Таким чином, власник може довести свої інтелектуальні права на зображення, пред'явивши секретний ключ, який використовувався для вбудовування мітки в зображення.

Даний водяний знак є напівкрихким: при внесенні змін до зображення з великою часткою ймовірності його можна буде ідентифікувати.

ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

Отже, одним із способів захисту авторського права на мультимедійну інформацію є застосування цифрових водяних знаків. Існують дві групи водяних знаків, впроваджуваних в зображення - це видимі (мікшування і нанесення тексту) і невидимі (LSB і Patchwork). Видимі водяні знаки являють собою певне викривлення зображення з метою інформувати користувача про автора або власника зображення. Невидимі водяні знаки служать для тих же цілей, але вони не видно неозброєним оком.

Ключові слова: цифровий водяний знак, інформаційний захист, мікшування, метод LSB, метод Patchwork.

ЛІТЕРАТУРА

1. Вовк О.О., Астраханцев А.А., Дорожан А.В. (2012) Исследование стойкости методов скрытия информации в неподвижных изображениях. Системи обробки інформації (науково-технічний журнал). Харків, 2 (54), 104-109.
2. Вовк О.О. (2011) Дослідження стійкості цифрових водяних знаків у відеофайлах і зображеннях. Наук. кер. А.А. Астраханцев. 15-й Международный молодежный форум «Радиоэлектроника и молодежь в XXI веке». Х.: ХНУРЭ, 4, 157-158.
3. Вовк О.О. (2011) Дослідження та порівняльна характеристика методів вбудовування інформації для прихованої передачі у мережах зв’язку. Наук. кер. А.А. Астраханцев. Інфокомунікації – сучасність та майбутнє: матеріали першої міжнародної науково-практичної конференції молодих вчених. Одеса, ОНАЗ, 1, 105-108.
4. Вовк О.О. (2012) Дослідження та порівняльна характеристика методів вбудовування інформації для прихованої передачі у мережах зв’язку. Наук. кер. А.А. Астраханцев. Підсумкова науково-практична конференція Всеукраїнського конкурсу студентських наукових робіт (галузь знань «Інформаційна безпека»). – Львів, ЛП.
5. Дорожан А.В., Астраханцев А.А., Вовк О.О. (2012) Исследование характеристик методов скрытия на основе НЗБ на фоне аддитивного шума. Вісник національного технічного університету «ХПІ», Харків, 18, 37-40.
6. Вовк О.О., Астраханцев А.А. (2014) Розроблення методики оцінювання важливості характеристик стеганографічних алгоритмів. Вісник національного університету «Львівська політехніка» «Інформаційні системи та мережі», Львів, 805, 52-60.